6. The method of claim 1 further comprising forwarding the access request to a regional LDAP database if the home region is LDAP enabled.

7. The method of claim 6 further comprising the regional LDAP database authenticating the user.

8. The method of claim 7 further comprising the regional LDAP database sending an "accept" message if the user is in the regional LDAP database and a "deny" message if the user is not in the regional LDAP database.

9. The method of claim 1 wherein the access request comprises a user name and password.

10. The method of claim 9 wherein the user name comprises a regional naming convention for identifying the home region of the user.

11. The method of claim 9 wherein the user name comprises an email address of the user.

12. the method of claim 9 further comprising comparing the user password to the password stored in the non-LDAP database.

13. The method of claim 12 wherein the password from the database is CHAP hashed, and wherein the password delivered to the database is CHAP hashed, and wherein the password comparison comprises comparing the CHAP hashed password delivered to the database with the CHAP hashed password extracted from the database.

14. The method of claim 12 wherein the database of the non-LDAP regions is an subscriber management system (SMS) database.

15. The method of claim 9 wherein the password is hashed to maintain security.

16. A system for dial roaming for users having a home non-LDAP region to allow access comprising:

a user computer having a home service region for creating a network access request;

a dial up connection over a first network to a network access server (NAS) in a roaming area:

a second network connected to the NAS for receiving the network access request;

a local network service provider connected to the second network;

a third network connected to the network service provider;

a corporate RADIUS server connected to the third network for receiving the access request; and

a regional LDAP server comprising a user database for authenticating the user access request and for allowing access to the regional network.

17. The system of claim 16 further comprising a regional RADIUS server connected to a non-LDAP regional server connected to the second network for receiving the access request.

18. The system of claim 17 wherein the non-LDAP regional server further comprises a user database and access instructions for authenticating the user access request in the non-LDAP server database.

19. The system of claim 18 wherein the database is an SMS database.

20. The system of claim 16 wherein the user access request comprises a user ID and password.

21. The system of claim 20 wherein the NAS further comprises instructions for hashing the user ID and password to enhance security.

22. The system of claim 18 wherein the non-LDAP server further comprises instructions to permit access if the user is in the database and to deny access if the user is not in the database.

23. A system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database comprising:

a RADIUS server, having a RADIUS authentication protocol, connected to a first network for receiving an access request from a user;

a subscriber management server, connected to a second network, comprising a user database for authenticating the user access request over the second network; and

a database view created in memory on the subscriber management server for providing user access information in the correct format for the RADIUS authentication protocol.

24. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 23 wherein the user access request is a username and password.

25. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 24 wherein the username is and email address.

26. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 24 wherein the

password from the user database is CHAP hashed to compare to the password presented in the user access request.

27. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 26 wherein the subscriber management server further comprises instructions for sending an "accept" message to the RADIUS server if the user password from the user database matches the user password presented in the user access request, and for sending a "deny" message to the RADIUS server if the user password from the user database does not matche the user password presented in the user access request.